

WHAT IS CLAIMED IS:

1. A method of transmitting contents information, comprising the steps of:
- 5 generating a first-key signal representative of a first key from first-key base information being a base of the first key;
- encrypting contents information into encryption-resultant contents information in response to the first-key signal;
- generating a second-key signal representative of a second key
- 10 on the basis of initial-value information of a given initial value according to a predetermined key generation algorithm;
- encrypting the first-key base information into encryption-resultant first-key base information in response to the second-key signal; and
- 15 transmitting the encryption-resultant contents information, the encryption-resultant first-key base information, the initial-value information, and algorithm identification information for identifying the predetermined key generation algorithm.
2. A method of recording contents information, comprising the steps of:
- generating a first-key signal representative of a first key from first-key base information being a base of the first key;
- encrypting contents information into encryption-resultant
- 25 contents information in response to the first-key signal;
- generating a second-key signal representative of a second key

09726423.120100

on the basis of initial-value information of a given initial value according to a predetermined key generation algorithm;

encrypting the first-key base information into encryption-resultant first-key base information in response to the second-key signal; and

recording the encryption-resultant contents information, the encryption-resultant first-key base information, the initial-value information, and algorithm identification information for identifying the predetermined key generation algorithm.

10

3. An apparatus for transmitting contents information, comprising:

means for generating a first-key signal representative of a first key from first-key base information being a base of the first key;

15 means for encrypting contents information into encryption-resultant contents information in response to the first-key signal;

means for generating a second-key signal representative of a second key on the basis of initial-value information of a given initial value according to a predetermined key generation algorithm;

20 means for encrypting the first-key base information into encryption-resultant first-key base information in response to the second-key signal; and

means for transmitting the encryption-resultant contents information, the encryption-resultant first-key base information, the
25 initial-value information, and algorithm identification information for identifying the predetermined key generation algorithm.

09725433.120100

4. An apparatus for recording contents information, comprising:
means for generating a first-key signal representative of a first
key from first-key base information being a base of the first key;

5 means for encrypting contents information into encryption-
resultant contents information in response to the first-key signal;

means for generating a second-key signal representative of a
second key on the basis of initial-value information of a given initial
value according to a predetermined key generation algorithm;

10 means for encrypting the first-key base information into
encryption-resultant first-key base information in response to the
second-key signal; and

means for recording the encryption-resultant contents
information, the encryption-resultant first-key base information, the
15 initial-value information, and algorithm identification information
for identifying the predetermined key generation algorithm.

5. A transmission medium for transmitting encryption-resultant
contents information, encryption-resultant first-key base
20 information, initial-value information, and algorithm identification
information, wherein the encryption-resultant contents information
and the encryption-resultant first-key base information are
generated by the steps of generating a first-key signal representative
of a first key from first-key base information being a base of the first
25 key; encrypting contents information into encryption-resultant
contents information in response to the first-key signal; generating

09726433-120100

a second-key signal representative of a second key on the basis of initial-value information of a given initial value according to a predetermined key generation algorithm; and encrypting the first-key base information into encryption-resultant first-key base information in response to the second-key signal; and wherein the algorithm identification information is for identifying the predetermined key generation algorithm.

6. A recording medium loaded with encryption-resultant contents information, encryption-resultant first-key base information, initial-value information, and algorithm identification information, wherein the encryption-resultant contents information and the encryption-resultant first-key base information are generated by the steps of generating a first-key signal representative of a first key from first-key base information being a base of the first key; encrypting contents information into encryption-resultant contents information in response to the first-key signal; generating a second-key signal representative of a second key on the basis of initial-value information of a given initial value according to a predetermined key generation algorithm; and encrypting the first-key base information into encryption-resultant first-key base information in response to the second-key signal; and wherein the algorithm identification information is for identifying the predetermined key generation algorithm.

7. An apparatus as recited in claim 3, wherein the means for

generating the second-key signal comprises a linear feedback shift register using a specified irreducible primitive polynomial.

8. A method of transmitting contents information, comprising
5 the steps of:

generating a first-key signal representative of a first key from
first-key base information being a base of the first key;

encrypting contents information into encryption-resultant
contents information in response to the first-key signal;

10 generating a second-key signal representative of a second key
on the basis of initial-value information of a given initial value
according to a predetermined key generation algorithm;

encrypting a part of the first-key base information in response
to the second-key signal to convert the first-key base information

15 into encryption-resultant first-key base information; and

transmitting the encryption-resultant contents information,
the encryption-resultant first-key base information, the initial-value
information, and algorithm identification information for identifying
the predetermined key generation algorithm.

20 9. A method of recording contents information, comprising the
steps of:

generating a first-key signal representative of a first key from
first-key base information being a base of the first key;

25 encrypting contents information into encryption-resultant
contents information in response to the first-key signal;

09726433.120100

generating a second-key signal representative of a second key on the basis of initial-value information of a given initial value according to a predetermined key generation algorithm;

5 encrypting a part of the first-key base information in response to the second-key signal to convert the first-key base information into encryption-resultant first-key base information; and

10 recording the encryption-resultant contents information, the encryption-resultant first-key base information, the initial-value information, and algorithm identification information for identifying the predetermined key generation algorithm.

10. An apparatus for transmitting contents information, comprising:

15 means for generating a first-key signal representative of a first key from first-key base information being a base of the first key;

means for encrypting contents information into encryption-resultant contents information in response to the first-key signal;

20 means for generating a second-key signal representative of a second key on the basis of initial-value information of a given initial value according to a predetermined key generation algorithm;

means for encrypting a part of the first-key base information in response to the second-key signal to convert the first-key base information into encryption-resultant first-key base information; and

25 means for transmitting the encryption-resultant contents information, the encryption-resultant first-key base information, the initial-value information, and algorithm identification information

for identifying the predetermined key generation algorithm.

11. An apparatus for recording contents information, comprising:
means for generating a first-key signal representative of a first
5 key from first-key base information being a base of the first key;
means for encrypting contents information into encryption-
resultant contents information in response to the first-key signal;
means for generating a second-key signal representative of a
second key on the basis of initial-value information of a given initial
10 value according to a predetermined key generation algorithm;
means for encrypting a part of the first-key base information
in response to the second-key signal to convert the first-key base
information into encryption-resultant first-key base information; and
means for recording the encryption-resultant contents
15 information, the encryption-resultant first-key base information, the
initial-value information, and algorithm identification information
for identifying the predetermined key generation algorithm.
12. A transmission medium for transmitting encryption-resultant
20 contents information, encryption-resultant first-key base
information, initial-value information, and algorithm identification
information, wherein the encryption-resultant contents information
and the encryption-resultant first-key base information are
generated by the steps of generating a first-key signal representative
25 of a first key from first-key base information being a base of the first
key; encrypting contents information into encryption-resultant

09726433.120100

contents information in response to the first-key signal; generating
a second-key signal representative of a second key on the basis of
initial-value information of a given initial value according to a
predetermined key generation algorithm; and encrypting a part of
the first-key base information in response to the second-key signal
to convert the first-key base information into encryption-resultant
first-key base information; and wherein the algorithm identification
information is for identifying the predetermined key
generation algorithm.

13. A recording medium loaded with encryption-resultant
contents information, encryption-resultant first-key base
information, initial-value information, and algorithm identification
information, wherein the encryption-resultant contents information
and the encryption-resultant first-key base information are
generated by the steps of generating a first-key signal representative
of a first key from first-key base information being a base of the first
key; encrypting contents information into encryption-resultant
contents information in response to the first-key signal; generating
a second-key signal representative of a second key on the basis of
initial-value information of a given initial value according to a
predetermined key generation algorithm; and encrypting a part of
the first-key base information in response to the second-key signal
to convert the first-key base information into encryption-resultant
first-key base information; and wherein the algorithm identification
information is for identifying the predetermined key generation

09726433.120100

algorithm.

14. An apparatus as recited in claim 10, wherein the means for generating the second-key signal comprises a linear feedback shift register using a specified irreducible primitive polynomial.

15. A method of decrypting encryption-resultant contents information generated by an encrypting side which implements the steps of generating a first-key signal representative of a first key from first-key base information being a base of the first key; encrypting contents information into encryption-resultant contents information in response to the first-key signal; generating a second-key signal representative of a second key on the basis of initial-value information of a given initial value according to a predetermined key generation algorithm; and encrypting the first-key base information into encryption-resultant first-key base information in response to the second-key signal; the method comprising the steps of:

- identifying the predetermined key generation algorithm in response to algorithm identification information for identifying the predetermined key generation algorithm;

generating a second-key signal representative of a second key on the basis of the initial-value information and the identified key generation algorithm;

- decrypting encryption-resultant first-key base information into original first-key base information in response to the second-key signal;

09726433.120100

generating a first-key signal representative of a first key from the original first-key base information; and

decrypting encryption-resultant contents information into original contents information in response to the first-key signal.

5

16. An apparatus for decrypting encryption-resultant contents information generated by an encrypting side which implements the steps of generating a first-key signal representative of a first key from first-key base information being a base of the first key;

10 encrypting contents information into encryption-resultant contents information in response to the first-key signal; generating a second-key signal representative of a second key on the basis of initial-value information of a given initial value according to a predetermined key generation algorithm; and encrypting the first-key base information
15 into encryption-resultant first-key base information in response to the second-key signal; the apparatus comprising:

means for identifying the predetermined key generation algorithm in response to algorithm identification information for identifying the predetermined key generation algorithm;

20 means for generating a second-key signal representative of a second key on the basis of the initial-value information and the identified key generation algorithm;

means for decrypting encryption-resultant first-key base information into original first-key base information in response to

25 the second-key signal;

means for generating a first-key signal representative of a first

09726433-120100

key from the original first-key base information; and
means for decrypting encryption-resultant contents
information into original contents information in response to the
first-key signal.

5

17. An apparatus as recited in claim 16, wherein the identifying
means comprises means for selecting one from among a plurality of
key generation algorithms in response to the algorithm
identification information as the identified key generation
10 algorithm.

18. An apparatus as recited in claim 17, wherein the means for
generating the second-key signal comprises a linear feedback shift
register having a feedback object position which is set in
15 accordance with a primitive polynomial in the identified key
generation algorithm.

19. A method of decrypting encryption-resultant contents
information generated by an encrypting side which implements the
20 steps of generating a first-key signal representative of a first key
from first-key base information being a base of the first key;
encrypting contents information into encryption-resultant contents
information in response to the first-key signal; generating a second-
key signal representative of a second key on the basis of initial-value
25 information of a given initial value according to a predetermined key
generation algorithm; and encrypting a part of the first-key base

09726433-120100

information in response to the second-key signal to convert the first-key base information into encryption-resultant first-key base information; the method comprising the steps of:

5 identifying the predetermined key generation algorithm in response to algorithm identification information for identifying the predetermined key generation algorithm;

generating a second-key signal representative of a second key on the basis of the initial-value information and the identified key generation algorithm;

10 decrypting encryption-resultant first-key base information into original first-key base information in response to the second-key signal;

generating a first-key signal representative of a first key from the original first-key base information; and

15 decrypting encryption-resultant contents information into original contents information in response to the first-key signal.

20. An apparatus for decrypting encryption-resultant contents information generated by an encrypting side which implements the
20 steps of generating a first-key signal representative of a first key from first-key base information being a base of the first key; encrypting contents information into encryption-resultant contents information in response to the first-key signal; generating a second-key signal representative of a second key on the basis of initial-value
25 information of a given initial value according to a predetermined key generation algorithm; and encrypting a part of the first-key base

09726433.120100

information in response to the second-key signal to convert the first-key base information into encryption-resultant first-key base information; the apparatus comprising:

means for identifying the predetermined key generation
5 algorithm in response to algorithm identification information for identifying the predetermined key generation algorithm;

means for generating a second-key signal representative of a second key on the basis of the initial-value information and the identified key generation algorithm;

10 means for decrypting encryption-resultant first-key base information into original first-key base information in response to the second-key signal;

means for generating a first-key signal representative of a first key from the original first-key base information; and

15 means for decrypting encryption-resultant contents information into original contents information in response to the first-key signal.

21. An apparatus as recited in claim 20, wherein the identifying
20 means comprises means for selecting one from among a plurality of key generation algorithms in response to the algorithm identification information as the identified key generation algorithm.

25 22. An apparatus as recited in claim 21, wherein the means for generating the second-key signal comprises a linear feedback shift

09726433.120100

register having a feedback object position which is set in accordance with a primitive polynomial in the identified key generation algorithm.

09726433.120100